The Importance of Manual Labor

March 2006

One moment you're fixing the company's DVD player and the next moment you're "volunteered" to be your unit's Network Administrator. You report for specialized training and are ushered into a room with a pile of manuals and a reading lamp. Soon you are seated in front of a computer and told, "Do your job soldier. We're counting on you."

In the pile of books you come across the DOD's newly issued information assurance manual, Information Assurance Workforce Improvement Program, DOD 8570.1-M. It requires services and Defense agencies for the first time to formally identify all employees with responsibility for any aspect of information assurance (IA), assign them positions within a new organizational structure and ensure that each worker has the certifications required for that position.

While you might have gotten this assignment because someone determined you were good with electronics –or maybe just killer at video games – you now have a security responsibility that is as important as any in the service. This is especially true if you're in the Sandbox.

The most valuable aspect of this manual is that it lays out an organized structure that will enable military personnel and the contractors that support them to be better organized, trained and prepared from the very real threats to the Global Information Grid. Attacks on our cyber infrastructure are constant, widespread, multi-sourced and increasingly sophisticated. Every soldier has a duty to protect this mission-critical resource, especially those who operate and maintain it.

Training to run a secure computer network, or take responsibility for any aspect of one, is as important as any ordnance or tactical training a soldier will ever have. The cyber perimeter is critical because once compromised it can threaten much more than even a breech of a camp perimeter. Cyber attacks are silent, stealthy and can result in loss of life just as much as an IED or a frontal assault.

Manuals are a necessary evil of coming up to speed on computers and networks, but those new to the game should seek out advice from more experienced personnel. Much as you would seek advice from a veteran of many engagements, network administrators should trade war stories as well in order to share a body of defensive knowledge that is critical to the operational safety of the Army.

In addition, combine what you pick up from that mountain of manuals with common sense. A network is to be guarded and protected much like any other high value resource such as a munitions storage area or strategic planning documents. The security of technical, physical and virtual keys is critical. Allowing unauthorized communications or activities that open networks to attack are as dangerous as dozing off on guard duty. While computers networks are complicated, the security procedures that protect them are not.

So take the title of Professor or Wirehead or Geek seriously. How you came into the position is less important than the job itself because you are now responsible for the information grid that protects and enables your fellow soldiers.